Queen's University Belfast

Security Policy User Guide 1

Data Encryption for QUB Confidential Data

Introduction

This document is targeted at those users working with QUB data classed as private/confidential and where the data will be used in a mobile environment.

It is compulsory to use data encryption on computers with data classed as confidential to make it very difficult for others to view that data without being granted access to it. This applies direct to devices such as notebook and other portable computers, on desktop computers containing sensitive information, and for sensitive data stored on media such as CD, DVD and memory sticks.

The purpose of the document is to define selected tools to satisfy the requirements of the QUB Security Policies on data handling using data encryption, and to highlight the difference in working practices that must be adopted to make successful use of data encryption methods.

Background

Data stored on computer media and computers can be protected in a number of ways. Passwords can be applied to systems, to user accounts, to collections of files and to individual files. In all cases, a determined data thief could easily recover the data, despite the password protection. A much better solution is to use data encryption, employing coding algorithms that are exceptionally difficult to break.

This document is concerned with data encryption, not password protection. It outlines the selected QUB tool for encryption services, addresses some of the issues surrounding encrypted data and highlights the main implications for business processes and working practices once encryption is adopted.

Important Points to Note

Before looking at the proposed encryption solution, it is worth highlighting some important points concerning data encryption.

Merely adapting encryption is not a panacea for all issues on security. To think that. encrypting all data and your worries are over, as far as loss or theft of the computer or media is concerned is incorrect unless users follow good working practice. Users must appreciate the following points and their consequences for data encryption to be successful.

1. A computer with encrypted data is only protected when it is fully switched off. When a computer is running, anyone can view its contents if they have access to the keyboard or screen. If a notebook computer is put into standby or hibernation mode, there are methods to access data and retrieve encryption keys, which can subsequently be used to open up the encrypted data.

   Good Practice

   Never leave a computer with encrypted data, especially a notebook computer, in standby or hibernation mode for any length of time when unattended. Always shut down the computer when it will not be used for a few hours, and especially overnight.

2. Data encryption can be applied to a whole disk, to a file used as an encrypted virtual disk, or to both. In all cases, a key (a strong password, strong pass phrase or a key on a USB memory stick) will be used to gain access to the encrypted data. Without these keys, it will be impossible to access the encrypted data and the data will not be viewable or recoverable. **There is normally no recovery from loss of keys, so be warned.** Additionally, if the whole disk is encrypted, a corruption of the loader pages or partition table or other disk sectors will usually render the data irretrievably lost.

   Good Practice

   Make a note of passwords or pass phrases and keep the information in a safe place or places. Certainly not on or about the computer, though. Encryption systems normally provide a facility to make recovery CDs. Users should make sure they do this, and keep these disks up-to-date if that is required. Recovery CDs help when there is corruption of the loader pages and, possibly, the partition table. Users should think carefully before using a USB memory stick to hold encrypted passwords, as these can be stolen or become corrupt. Copies of memory sticks help in the latter situation. A stolen memory stick may be used to gain access to encrypted data, unless keys are changed after the loss is noted. See appendix 1 for advice on passwords.

A virtual encrypted disk, contained in a file, is normally not accessible, even if the whole disk has been encrypted, until such times as it is mounted as a disk and assigned a drive letter (R:, say). When dismounted after use, the data becomes inaccessible once more. Users should consider using one of these virtual disks to hold very sensitive information, as the technique provides two layers of key and encryption protection.

3. Users should make copies of all their important data, both before employing encryption and then regularly thereafter.

   Good Practice

   If a computer is stolen, if its disk fails or if data corruption occurs, such that the data cannot be recovered, having one or more copies of data allows a swift recovery from a very damaging position. Normal data-recovery tools usually cannot be applied to an encrypted disk or file, so secure data backup becomes even more important when data encryption is employed.

4. The way a disk is partitioned can be very important. If a disk contains one partition only, holding the operating system, applications and data, anything causing a failure of that partition will inevitably cause loss of the data, unless the recovery disks can successfully decrypt the disk. Even then, data recovery may be impossible. If the operating system and applications are on one partition and the data on another partition, loss of the partition holding the operating system will normally not affect the data partition. Hence, the data can be recovered. However, damage to the data partition may cause loss of all data (hence the reason for backups).

   Good Practice

   Where possible, and mostly it is, keep data in its own partition, separate from the operating system and applications. For Windows computers, this means storing Windows in the C: drive and data in a D: drive, say.

Data Encryption Methods (Hardware & Software)

A number of methods exist whereby data on computers and media can be encrypted. Most of these methods are software based, although a few hardware-based solutions exist. The hardware-based solutions normally comprise a disk that has data encryption algorithms built into the drive itself. Such a drive is faster than a normal disk drive coupled to encryption software, but the software solution is not much slower.

Of particular interest, perhaps, are USB memory pens that have proper encryption techniques built in to them. These devices require no external drivers or software to

be installed on a computer. Everything is self-contained, and the devices can be used by simply plugging them into a free USB port and quoting the security password for the key. They use a Trusted Platform Module chip (see next paragraph) to generate and store keys.

For a few years, computers have been appearing that contain a Trusted Platform Module (TPM) chip. This is a secure cryptoprocessor chip containing a pseudo random number generator, used in deriving cryptographic keys, and capable of storing them very securely. A combined TPM and software solution is generally stronger than a software only solution, but a TPM system can be compromised under a special condition, which thankfully is unlikely to apply in most instances. It follows, therefore, that all notebook computers should now be purchased with a TPM processor, until further notice.

A notebook computer with encryption inbuilt in the hard disk is secure from the outset and needs no further work to make it secure. Notebook computers with a non-encrypting disk can be converted to be partially or fully encrypted, by applying one of a number of software solutions. In extremis, it is possible to discover cryptographic keys written to parts of the disk, such as the swap area, when full disk encryption is not employed. To safeguard this possibility, full disk encryption is recommended.

QUB Selected Tool for USB Pen Based Encryption

A small number of USB pens have appeared that contain everything to provide data encryption on the drive itself, independent of the computer it is attached to. These devices are ruggedized, come in a range of versions and sizes (personal, business, military) and operate AES 256-bit encryption. IronKey is the preferred device for QUB, however this is currently an expensive solution. A review of the many options has identified that the best solution is where the device has hardware encryption. The next best device is a SanDisk Cruzer Enterpirse device, roughly 30% cheaper than the Ironkey.

The Ironkey provides a very rugged casing, which is waterproof. The IronKey electronics are well shielded and enclosed in an epoxy potting compound. This renders virtually impossible the successful extraction of the electronics for investigative and data recovery work. The device will also securely destroy all data, keys and passwords if 10 consecutive, unsuccessful attempts are made to gain access to the data.

At present, the IronKey range requires Windows 2000, Windows XP or Windows Vista to initialise them. Thereafter, an IronKey device can also be used on a Mac or Linux computer. IronKey are working on a Mac compatible version, so take it that Mac is not yet a usable platform. IronKey comes in Basic, Individual and Enterprise models. The Basic model cannot be updated with later versions of software, amongst other things, compared to the Enterprise model.

The SanDisk option is not as rugged as the Ironkey with slightly less management functionality but will still meet the data security requirements.

These memory pens are well suited for the storage of data in a secure environment, where the loss or theft of the device will not result in the data being recovered. However, some information may be recoverable from computer memory and disk swap areas if access to a computer, used to host the device, is possible. Despite this mild threat, these memory pens offer a very good solution for data protection.

Such devices are not cheap at present, the smallest (1GB) and cheapest costing about £45 - £50. This must be offset against the cost of dealing with the disclosure of the data in the event of a normal memory pen being lost or stolen.

Finally, there is nothing to prevent these memory pens being used with computers already encrypted with TrueCrypt software solution.

Regular backup of data is essential when using any encryption product. Ironkey has a backup feature to allow an encrypted copy of the data to be safely stored in regular file space. The copy can be used to restore the data and for backup to a new IronKey device.

QUB Selected Tool for Software Based Encryption

The selected solution for QUB is TrueCrypt which provides on-the-fly encryption and decryption of data. Unencrypted data is never stored in memory: data is always stored on disk in encrypted form.

When using this encryption tool, please, please, please note all the warnings about making regular backup copies of data, about making and keeping recovery CDs up to date, and about storing passwords and passphrases safely. Failure to do all or any of these things may render your data inaccessible. Forever.

It should be noted that TrueCrypt, on occasions, offer the facility to view passwords as they are typed. This is counter to all security instructions you will ever have read. The purpose of the feature is to allow a user to validate a very long password or phrase, especially when setting the system up. It goes without saying that this facility should only be used when privacy is ensured.

TrueCrypt Overview

TrueCrypt is OpenSource software and is free. It is now available for Mac and Linux, as well as Microsoft Windows, and it is claimed that data stored in a virtual disk, housed in a file, can be easily transported from one system to another. Unfortunately, this claim could not be verified at moment, due to lack of suitable systems

Cost

Free (£0)

Installation

Installation is quick and easy

Generation of Encryption Keys

Although the system will generate encryption keys without intervention, some user input helps develop a set of cryptographically stronger keys. This involves moving the mouse around for about 30 seconds.

Key Storage

Keys are stored on the encrypted volume and on the recovery disk.

Authentication

Users authenticate to the system or a virtual disk by quoting a pass phrase and possibly specifying one or more keyfiles. Keyfiles are just ordinary files but they must be present if the 'Use Keyfiles' box is checked. They provide a two-factor authentication system. Keyfiles can be stored on fixed disks or USB memory devices.

The longer the pass phrase or password the better, but a user must make a safe note of it beforehand, as forgetting a password will prevent use of the system and total loss of the data.

Encryption

A user can choose to encrypt a new file (virtual disk or volume), a partition, a complete disk or a USB memory stick. A CD or DVD cannot be encrypted directly, but a virtual volume stored in a file can be written to CD or DVD. If encrypting a complete disk under Windows, the software will not proceed if a logical partition exists on the disk. Only primary partitions can be encrypted in this case. Thereafter, extended partitions must not be created, only primary partitions.

Encryption is a lengthy process, taking several hours, although the actual time required depends on the size of the disk. The encryption process can be interrupted and normal work can usually proceed in parallel. Given the nature of data encryption and the time required to

complete the task, it is better to ensure that the notebook computer is running on mains electricity and has a fully charged battery (in case of mains failure) before starting encryption.

Creating and encrypting a file to act as an encrypted virtual volume is usually a much quicker process.

Decryption

A whole disc can be decrypted, either from Windows or through use of the recovery CD. The process is much quicker when run from Windows. To decrypt a virtual volume, simply move all files to unencrypted disk space. The old virtual volume should then be formatted, to destroy the data, and the containing file deleted.

Recovery disk

The encryption process forces this to be made before proceeding with the encryption process, which is a very good thing. The key password or phrase is stored on the disk in encrypted form. The disk allows repair of the TrueCrypt Boot Loader and the key data.

WARNING (from the Manual): By restoring key data using a TrueCrypt Rescue Disk, a user also restores the password that was valid when the TrueCrypt Rescue Disk was created. Therefore, whenever a user changes the password, they should destroy their TrueCrypt Rescue Disk and create a new one (select System -> Create Rescue Disk). Otherwise, anyone knowing the old password (for example, captured by a keystroke logger) and having access to the old TrueCrypt Rescue Disk, could use it to restore the key data (the master key encrypted with the old password) and thus decrypt your system partition/drive.

Ease of use

Once a disc is encrypted, TrueCrypt is transparent in use, except when starting or rebooting the computer. At this stage, which is pre-boot, a key password or phrase has to be entered and recognised before the boot process will continue.

Performance

No noticeable degradation in performance was detected in normal use, so degradation is mild. Encrypting the whole disk with TrueCrypt seemed slightly quicker than when using PGP WDE, but parameters can be set for WDE to increase or reduce speed. Its parameters were set for safety which increases the time required. Encryption of the whole drive can be interrupted and resumed.

Recovering from disk failure

TrueCrypt offers a few more possibilities than PGP WDE and these proved very worthwhile. Even when the Master Boot Record was wiped

clean, the recovery disk allowed the TrueCrypt loader to be reinstalled. It also allowed the disk to be decrypted. Then, using other tools, the partition table was reconstructed and both the operating system partition and data partition were recovered.

When the Windows loader page was corrupted, the recovery disk again allowed both partitions to be recovered. Reinstating the Windows loader page then allowed Windows to work again.

Virtual disks

These worked well. A file must be matched to an unassigned drive letter and then mounted, before the contents become available. The process is not as smooth as PGP WDE, where a virtual disk is assigned a drive letter at creation time, but it is not arduous and provides greater flexibility in choice of drive letter. It is straightforward to copy such files to a writable DVD, especially when the DVD is formatted with UDF (Universal Disk Format). New data could then be added directly to the virtual drive on DVD.

Importantly, there is nothing to indicate that a file contains a virtual drive, so anyone accessing the computer without permission, or reading a directory of a USB memory stick or DVD disk, would not easily discover it.

A portable version of TrueCrypt can be installed on a USB memory stick, along with a virtual volume. The data can then be viewed on a system that does not have TrueCrypt installed. The key password must be quoted before the encrypted data can be viewed.

Overall

TrueCrypt seems to offer a good level of performance, and data recovery was very good. The use of a DVD to hold a virtual drive that can easily be added to is a useful facility. The system seems secure in operation. Virtual volumes, by virtue of looking like ordinary files in a directory listing, are much more difficult to spot, should an unauthorised person manage to gain access to the system.

Appendix 1 Password Guidance

While a 6 to 8 character password is acceptable for logging into Queen's services, this is not the case for mobile devices with data encryption.

The main network will monitor for suspicious activity where password hacking is attempted. However, a device in stand alone mode can be hacked at leisure.

For a laptop with encryption, a much more complex password must be used. Many people believe that it is impossible to remember anything longer than an 8 digit password, but there are many approaches that support longer passwords.

1 – An old address, or family member address which may not be known by anyone.

33laganside paradebelfastnorthernirelandbt31az

2 – Multiple dates of birth for say four children or parents and siblings:

150819892903199131101993031019 97

3 – First line of a favourite song, poem or story:

alongtimeagoinagalaxyfarfaraway

These are 30+ character sequences that are easily remembered but almost impossible to hack. Combinations of the above can be used and to make passwords even more complex – for example, the strings can have "0" and "o", "3" and "e", "5" and "s" characters transposed.